What Is Claimed Is:

1. A method for verifying that a user is licensed to access digital content within a content file comprising:
   a) obtaining a product ID from the content file;
   b) comparing the product ID from the content file with a second product ID found in a product license;
   c) obtaining a user ID from the product license; and
   d) comparing the user ID from the product license with a second user ID found in a user license.
2. The method of claim 1, wherein the user license further contains personal information that is accessible to the user, such that the user would be reluctant to share the user license with other users.
3. The method of claim 2, wherein the personal information is a financial access number allowing access to financial resources of the user.
4. The method of claim 3, wherein the financial access number is a credit card number.
5. The method of claim 3, wherein the financial access number is of a type chosen from the following set: a bank account number, a gift certificate number, a debit card number, and a stored value card number.
6. The method of claim 1, further comprising:
   e) obtaining identifying system information from the user license; and
   f) comparing the identifying system information from the user license with identifying information obtained from a computer operating system being used by the user to access the digital content.
7. The method of claim 1, further comprising:
   e) allowing access to a first portion of the digital content when the comparisons of step b) and d) both result in successful comparisons.

8. The method of claim 7, further comprising:

f) allowing access to a second portion of the digital content when either of the comparisons of step b) and d) are not successful.

9. The method of claim 8, wherein the first portion of the digital content is encrypted and the second portion of the digital content is not encrypted.

10. The method of claim 7, wherein the first portion of the digital content is encrypted using a product encryption key.

11. The method of claim 10, wherein the product encryption key is found in the product license.

12. A method for allowing a user on a computer to access encrypted digital content found in a content file comprising:

a) accessing the content file to determine a product identifier found within the content file;

b) finding an appropriate product license that has the same product identifier as that found in the content file, the appropriate product license being located in a storage area accessible by the computer;

c) accessing the appropriate product license to determine a licensed user identifier associated with the product license;

d) finding an appropriate user license that has the same user identifier as that found in the appropriate product license;

e) accessing the appropriate product license to determine a decryption key associated with the product license; and

f) decrypting the encrypted digital content using the decryption key.

13. The method of claim 12, wherein non-encrypted data is found in the content file containing the encrypted digital content, and further wherein the non-encrypted data is accessible when the appropriate product license or the appropriate user license is not found.

14. The method of claim 13, wherein an option to purchase full access rights to the encrypted digital data is presented to the user when the appropriate product license or the appropriate user license is not found.

15. A method for registering digital content found at a first location with a remotely located license generator over a network comprising:

a) creating a session encryption key at the first location;

b) encoding the session encryption key using a public key of the remotely located license generator;

c) transmitting the encoded session encryption key and information relating to the digital content from the first location to the remotely located license generator over the network;

d) decoding the session encryption key using a private key of the license generator;

e) generating a content identifier at the license generator;

f) associating the content identifier with the information relating to the digital content;

g) encrypting the content identifier using the session encryption key;

h) transmitting the encrypted content identifier to the first location over the network; and

i) decrypting the content identifier using the session encryption key.

16. The method of claim 15, wherein the network is a public network.

17. The method of claim 16, wherein the public network is the Internet.

18. The method of claim 15, wherein the content identifier and the information relating to the digital content is associated in a database accessible by the remotely located license generator.

19. The method of claim 15, further comprising:

j) combining the content identifier with the digital content in a single file.

20. The method of claim 15, further comprising:

j) generating a product encryption key at the license generator when the content identifier is generated in step e);

k) associating the product encryption key with the content identifier; and

l) transmitting the product encryption key to the first location over the network.

21. The method of claim 20, wherein the product encryption key is encrypted using the session encryption key before the step of transmitting the product encryption key, and wherein the product encryption key is decrypted after the transmitting step.

22. The method of claim 20, further comprising:

m) combining the content identifier with the digital content in a content file; and

n) encrypting at least a portion of the digital content in the content file using the product encryption key.

23. The method of claim 22, wherein at least a portion of the content file is unencrypting, further comprising:

o) allowing access to the unencrypted portions of the content file when a the first location does not have access to a product license associated with the content identifier; and

p) allowing access to the encrypted portions of the content file when the first location does have access to a product license associated the content identifier.

24. A method for encrypting digital content found at a first location using a product encryption key generated at a second location via communications over a computer network; the method comprising:

a) creating a session encryption key at the first location;

b) encoding the session encryption key using a public key;

c) transmitting the encoded session encryption key and information relating to the digital content from the first location to the second location over the network;

d) decoding the session encryption key using a private key;

e) generating a product encryption key at the second location;

f) associating the product encryption key with the information relating to the digital content;

g) encrypting the product encryption key using the session encryption key;

h) transmitting the product encryption key to the first location over the network;

i) decrypting the product encryption key using the session encryption key; and

j) encrypting at least a portion of the digital content with the product encryption key.

25. The method of claim 24, wherein the product encryption key and the information relating to the digital content is associated in a database.

26. A method of obtaining a product license for digital data, where the product license is associated with a user and is obtained from a remote license generator over a computer network, the method comprising:

a) obtaining a user license from the remote license generator over the computer network, the user license containing a user identifier that uniquely identifies the user to the remote license generator;

b) storing the user license at a location that allows the user to retrieve and examine the user license without further interaction with the remote license generator;

c) ascertaining a product identifier from the digital data;

d) sending a request for the product license from the user to the remote license generator over the network, the request including the product identifier and the user identifier;

e) generating the product license at the remote license generator, the product license containing the product identifier and the user identifier;

f) transmitting the product license over the network back to the user; and

g) storing the product license at a location that allows the user to retrieve and examine the product license without further interaction with the remote license generator.

27. The method of claim 26, wherein step d) further includes the following substeps:

i) generating a session key;

ii) encrypting the session key using a public key associated with the remote license generator;

iii) transmitting the encrypted session key with the request for the product license.

28. The method of claim 27, wherein step f) further includes the following substeps:

i) decrypting the session key using a private key associated with the remote license generator;

ii) encrypting the product license using the session key; and

iii) transmitting the encrypted product license to the user over the network;

and further wherein the product license is decrypted by the user using the session key before the product license is stored in step g).

29. The method of claim 26, wherein the digital data is encrypted using a unique encryption key known to the remote license generator, and further wherein

the product license generated by the remote license generator includes the unique encryption key for the digital data.

30. The method of claim 29, wherein step d) further includes the following sub-steps:

    i) generating a session key;

    ii) encrypting the session key using a public key associated with the remote license generator;

    iii) transmitting the encrypted session key with the request for the product license.

31. The method of claim 30, wherein step f) further includes the following sub-steps:

    i) decrypting the session key using a private key associated with the remote license generator;

    ii) encrypting the product license using the session key; and

    iii) transmitting the encrypted product license to the user over the network;

and further wherein the product license is decrypted by the user using the session key before the product license is stored in step g).

32. A method for authorizing user access to a system for licensing digital data, the method comprising:

    a) receiving data over a computer network from the user including identifying information and confidential payment data;

    b) assigning a user identification to the user;

    c) storing the user identification, the identifying information and the confidential payment data in a central user database;

    d) storing the user identification, the identifying information, and the confidential payment data as a user license at a location accessible to the user without further interaction with the central user database;

e) accessing a product specific license when the user wishes to access a product, the product specific license containing a licensed user identification; and

f) comparing the licensed user identification with the user identification found in the user license for the user.

33. The method of claim 32, further comprising:

g) showing the confidential payment data found in the user license to the user at a time after the initial storing of the user license in step d), so as to discourage the sharing of a user license with other users.

34. A method for managing licenses for digital data comprising:

a) assigning a vendor ID to owners of rights in digital data;

b) registering a collection of digital data as a product with a product database, and assigning a product ID and an encryption key to the product;

c) storing the product ID and the encryption key with the vendor ID in the product database;

d) encrypting at least a portion of the collection of digital data with the encryption key, and

e) storing the encrypted digital data and product ID in a product file.

35. The method of claim 34, further comprising:

f) assigning a user ID to a user who desires access to the encrypted digital data;

g) storing the user ID and a payment mechanism in a user database; and

h) storing the user ID and the payment mechanism electronically as a user license such that the user can access the user license without referring to the user database.

36. The method of claim 35, further comprising:

i) receiving a request from the user to purchase access to the product file, the request including the product ID and the user ID;

j) verifying that the product ID is found in the product database and the user ID is found in the user database;

k) using the payment mechanism stored in the user database with the user ID to secure payment;

l) storing the user ID and the product ID in a product license database; and

m) storing as a product license the encryption key associated with the product ID in the product database along with the user ID and the product ID, such that the user can access the product license without referring to the product license database.

37. The method of claim 36, further comprising:

n) in response to a request by the user to access the product file, searching for the product license containing the product ID of the product file;

o) comparing the user ID in the found product license with the user ID found in an accessible user license;

p) using the encryption key in the found product license to decrypt the encrypted digital data found in the product file.

38. The method of claim 37, wherein the product database, the user database, and the product license database are combined into a single database.

39. A system for managing licenses to digital data comprising:

a) a producer software program for encrypting digital data and including with the encrypted digital data a product identifier;

b) a player software program capable of decrypting the encrypted digital data, the player software having associated with it

i) at least one product license having a product identifier, a user identifier, and a decryption key; and

ii) a user license having a user ID.

40. The system of claim 39, wherein the player software is able to purchase additional product licenses, and further comprising:

c) a license provider having a database of products, users, and product licenses, wherein

i) the database of products contains multiple entries, with each entry having the product identifier, a vendor identifier, and a decryption key,

ii) the database of users contains multiple entries, with each entry having a user identifier and a mechanism for payment by the user, and

iii) the database of product licenses contains multiple entries, with each entry having a product identifier and a user identifier.